JP92000-0134

J1046 U.S. PTO
09/884672
06/19/01

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

#4

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ６月２０日

出 願 番 号
Application Number: 特願２０００－１８４６９７

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレーション

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願

【整理番号】　JP9000134

【あて先】　特許庁長官殿

【国際特許分類】　H04L 12/46

H04L 12/28

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　野口　哲也

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　東京基礎研究所内

【氏名】　下遠野　享

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【弁理士】

【氏名又は名称】　渡部　弘道

【復代理人】

【識別番号】　100060726

【弁理士】

【氏名又は名称】　石山　博

【選任した復代理人】

【識別番号】　100085408

【弁理士】

【氏名又は名称】　山崎　隆

【手数料の表示】

【予納台帳番号】　006091

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9706050

【包括委任状番号】　9704733

【包括委任状番号】　0004480

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アドホック無線通信用検証システム

【特許請求の範囲】

【請求項１】　アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていることを特徴とするアドホック無線通信用検証システム。

【請求項２】　前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項１記載のアドホック無線通信用検証システム。

【請求項３】　検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていることを特徴とする請求項１記載のアドホック無線通信用検証システム。

【請求項４】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされることを特徴とする請求項１～３のいずれかに記載のアドホック無線通信用検証システム。

【請求項５】　前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１～３のいずれかに記載のアドホック無線通信用検証システム。

【請求項６】　関数を演算子、該演算子が作用する数値を該演算子の入力、

該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項５記載のアドホック無線通信用検証システム。

【請求項７】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項５記載のアドホック無線通信用検証システム。

【請求項８】　前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項１～７のいずれかに記載のアドホック無線通信用検証システム。

【請求項９】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項８

記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

【請求項１０】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項８記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

【請求項１１】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項１２】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項１３】　アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていることを特徴とするアドホック無線通信用検証方法。

【請求項１４】　前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項１３記載のアドホック無線通信用検証方法。

【請求項１５】　検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていることを特徴とする請求項１３記載のアドホック無線通信用検証方法。

【請求項１６】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検

証データとされることを特徴とする請求項１３～１５のいずれかに記載のアドホック無線通信用検証方法。

【請求項１７】　前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１３～１５のいずれかに記載のアドホック無線通信用検証方法。

【請求項１８】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１７記載のアドホック無線通信用検証方法。

【請求項１９】　関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていることを特徴とする請求項１７記載のアドホック無線通信用検証方法。

【請求項２０】　前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項１３～１９のいずれかに記載のアドホック無線通信用検証方法。

【請求項２１】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方

のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項２０記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項２２】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とする請求項２０記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項２３】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、

公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項２４】　各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項２５】　次の内容のアドホック無線通信用検証システム用プログラムを記録した記録媒体。

：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようにな

っている。

【請求項２６】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５記載の記録媒体。

：前記検証データは、視覚的又は聴覚的な検証データである。

【請求項２７】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５記載の記録媒体。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【請求項２８】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５～２７記載の記録媒体。

：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【請求項２９】　次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項２５～２７記載の記録媒体。

：前記第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【請求項３０】　次の内容のアドホック無線通信用検証システム用プログラムを配信する配信装置。

：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、伝送データの改ざんに対処するアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置に関するものである。

【０００２】

【従来の技術】

アドホック無線通信のような特定のインフラを利用しないその場限りの近距離無線通信において不特定の二者が、データを悪意の第三者により改ざんされることなく、伝送する場合には、悪意の第三者に知られることにない暗号鍵を共有する必要がある。しかしながら、通信時に随時その暗号鍵の基となる値を設定する方法は煩雑であり、特に通信相手が初顔合わせ等の状況下では、通信相手同士が口頭やメモ等により暗号鍵を交わすことはほとんど実用性がない。自動的に暗号鍵を共有する方法として，まず公開鍵を共有して，暗号鍵をその公開鍵で暗号化して共有する方法がある。しかし、マン・イン・ザ・ミドル・アタック（Man-in-the-middle attack：マン・イン・ザ・ミドル・アタックの詳細については、ジョン・ウィリィ・アンド・サンズ会社(John Wiley & Sons,Inc)出版の著者ブルース・シュナイアー（BRUCE SCHNEIER）の題名：応用暗号学（APPLIED CRYPTOGRAPHY）のｐ．４８～ｐ．５０を参照されたい。）のリスクがある。

【０００３】

マン・イン・ザ・ミドル・アタックにおけるデータ改ざんのリスクを概略する。図１はアドホック無線通信システム１０において送信元Ａと送信先Ｂとが気付かないままで両者の間に悪意の第三者Ｃが介在する余地を示している。ＡとＢとは、（ａ）のように、両者間に直接、通信路が開設されていると、思っていても、（ｂ）のように、実は第三者が両者の間に割り込んでいる場合がある。"Man-in-the-Middle Attack"がどのように実行されるのか、具体的に例を挙げて説明する。

【０００４】

無線暗号通信路開設の一般的な手順は以下のようになる。

手順１：送信元は不特定多数の相手に向かって、通信したい送信先のＩＤで呼びかける。

手順２：送信先が無線接続可能な範囲に居れば、その呼びかけられたＩＤ（つまり自分のＩＤ）を受信する。

手順３：送信先は、自己の動作条件等を送信元に伝える。

手順４：通信路開設のために必要な動作パラメータ（利用する通信路の選択と設定、暗号鍵の交換等）を両者で決定する。

手順５：通信路開設し、相互交信が開始される。

【０００５】

悪意の第三者が図１のＣの位置に最も入り込み易いのは、盗聴の対象となる二者が対面で無線通信を開始するタイミングである。つまり、上記の列挙された手順１～３に介入する。図２及び図３は悪意の第三者が図１のＣの位置に入り込む手口の一例を示す。電波の性格上、送信元Ａは周囲のすべての送信先候補に特定ＩＤで呼びかけざるを得ない（手順１）。送信先Ｂは、自分のＩＤでの呼びかけが聞こえるので（手順２）、送信元Ａに応答する（手順３）。ここで、悪意の第三者は自分以外のＩＤへの呼びかけに応答したり、自分以外のＩＤで呼びかけを行ったりして、下記のような成りすましを図ろうとする。まず、悪意の第三者Ｃは送信先Ｂの応答に同一周波数帯のノイズをぶつけて送信元Ａがその応答を聞き取れないようにする。この時点で、送信先Ｂはそのノイズの事実を知らないので、上記手順４に遷移して送信元Ａからの手順４におけるセッション開始を待っている。送信元Ａは手順４には居ないので、送信先Ｂはタイムアウト後に再度、自分のＩＤの呼びかけを聞く状態に戻る。一方、送信元Ａは送信先Ｂからの応答が得られないので、タイムアウト後に再度同じＩＤで呼びかける（手順１）のが普通である。つまり、送信元Ａと送信先Ｂは互いの手順の同期を取り始めようとして、それぞれのタイムアウトでその失敗に気がつき、元の状態に戻ることになる。

【０００６】

悪意の第三者Ｃは、送信元Ａが再度同じＩＤで呼びかけるタイミングに合わせて待機し、さらに送信先Ｂが再度自分のＩＤの呼びかけを聞き始めるタイミングにも合わせて待機する。以後、悪意の第三者Ｃは送信元Ａの呼びかけに送信先Ｂに成りすまして応答し、反対に自分のＩＤの呼びかけを聞き始めた送信先Ｂに送信元Ａに成りすまして呼びかけを行う。勿論、悪意の第三者ＣはどのようなＩＤにも自分のＩＤを変化させる能力を用意している。上記で送信元Ａと送信先Ｂが互いの手順の同期はずれから元の状態に戻るのは同一時刻ではないので、このような二つの成りすまし行為を悪意の第三者Ｃは実行可能である。なぜなら、送信元Ａと送信先Ｂがそれぞれ次のイベントで待機し始める時刻がそもそも異なるし、タイムアウトの対象となるイベントも異なるのでタイムアウト期間自身も異なるからである。

【０００７】

この成りすまし工作によって、送信元Ａは、正規の送信先Ｂから正常な応答があったと思って、通信路開設手順、つまり手順４より悪意の第三者Ｃと一緒に遷移するし、送信先Ｂは、正規の送信元Ａからの呼びかけだと思って、通信路開設手順に同じく第三者Ｃと一緒に遷移する。上記手順５まで進むと、二者のみで通信路を確保したと思っている両者Ａ、Ｂの機器の保有者に知られることなく悪意の第三者Ｃが互いの間で通信データを中継する形で盗聴することが可能になる。この成りすまし（中継）を利用すれば、例えばＡがＢに送るはずの公開鍵をＣが改ざんして、Ｃが予め用意した秘密鍵に対応した公開鍵とすり替えることができる。これによって、本来ＡとＢの間で構築される暗号通信路はＡとＣの間でのみ有効になり、ＣとＢとの間はＣが別に設定した暗号通信路となる。つまり、Ａから送られた暗号化データはＣで復号化され、再度ＣとＢの間の暗号化通信路用に別の暗号化を適用されて伝送される。その逆の伝送も同様である。ＡとＢは共に通常手順で暗号化通信路を確立していながら、途中で公開鍵をすり替えられ、そのすり替えに気がつかないことで、盗聴される結果となる。このような攻撃（成りすましによる盗聴）をMan-in-the-middle attackと呼ぶ。暗号化通信路自身は安全であるから、このような攻撃への対処として、通信する両者で本当に同一の公開鍵を共有しているか否かを確実にすることが肝要となる。

【０００８】

【発明が解決しようとする課題】

Man-in-the-middle attackの対処法としては、認証機関の発行する証明書を利用して、証明書内に記載された個人ＩＤ（通常相手の名前等）を伝送元、伝送先で表示し目視比較することも考えられる。しかし、これには、証明書の発行にコストがかかる。また、認証機関を利用する場合、身元を登録して認証を行うため、通信相手に自分の身元を公開することになり、匿名性を保つことができないという問題も存在する。さらに、イエローページ（Ｙｅｌｌｏｗ　Ｐａｇｅ）のように公開鍵から利用者を特定するサービスを用いる場合は、電話回線等によるセキュアなネットワーク接続が必要であり、トランザクションコストがかかる。

【０００９】

本発明の目的は、アドホック無線接続により相互に接続されるデータ送受装置間でデータを送受する場合において、通信相手へのなりすましによるデータの改ざんを有効に防止できるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。

本発明の他の目的は、口頭やメモ書きによるパスワードの取り交わしを省略でき、身元公開してしまう認証機関を利用せず、能率的に、円滑に、かつ正確に通信相手を検証することのできるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。

【００１０】

【課題を解決するための手段】

本発明のアドホック無線通信用検証システム及び方法によれば、アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証

データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【００１１】

両データ送受装置の距離は、両データ送受装置の検証データ出力部における検証データを相互に対比する必要があるので、典型的には、両データ送受装置間をユーザ（利用者）が数秒で行き来できる１０ｍ以内等であり、好ましくは数ｍである。検証データ生成用データに基づいて生成した検証データには検証データ生成用データそのものであってもよいとする。検証データは、両データ送受装置の検出データ出力部における検証データが相互に一致しているか否かの判定が行い易いものに設定される。一般には、両データ送受装置において起動されている検証用ソフトが同一であれば、検証データ生成用データから検証データの生成のために同一の生成アルゴリズムが使用される。しかし、複数個の生成アルゴリズムの内の１個を、両データ送受装置のユーザがその場において適宜、取り決めたりするようになっていてもよい。

【００１２】

一方のデータ送受装置は、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて検証データを生成する。他方のデータ送受装置は、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて検証データを生成する。そして、両データ送受装置の検出データ出力部から出力される検証データが一致するか否かの判定を行い、一致していれば、検証データ生成用データが、途中において改ざんされることなく、一方のデータ送受装置から他方のデータ送受装置へ正しく伝送されていること、すなわちデータ完全性が検証されたことになる。このように、データ完全性の検証を能率的に実施できる。

【００１３】

本発明のアドホック無線通信用検証システム及び方法によれば、検証データは、視覚的又は聴覚的な検証データである。

【００１４】

視覚的な検証データには、画像、数値、文字、又はそれらの組み合わせがある。検証データの視覚表示の例としては、検証データが例えば計ｎビットのビットデータである場合に、ｎビットを、連続する等ビットずつで区分し、ｘ軸方向へ区分、ｙ軸方向へ各区分ごとの数量とするヒストグラムがある。検証データの聴覚表示の例としては、前述のヒストグラムの各区分の数量に対応する高さの音を、低位の区分から順番に出力するものである。検証データは、両データ送受装置における検証データの一致及び不一致をユーザが円滑かつ正確に判定し易いものが選択されるのが好ましい。

【００１５】

本発明のアドホック無線通信用検証システム及び方法によれば、検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていること。

【００１６】

検証データの視覚的出力形態では、両データ送受装置におけるもの同士が類似していても、検証データの聴覚的出力形態では相違が明確であり、あるいはその逆の場合がある。検証データの視覚的出力形態及び聴覚的出力形態の両方が対比されることにより、一致及び不一致の判定の正確性が高まる。

【００１７】

本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【００１８】

一方向性関数には例えばハッシュ関数（Ｈａｓｈ　Ｆｕｎｃｔｉｏｎ）がある。上記定義した演算子列には、演算子が１個しかないものも含んでいる。検証データ生成用データからの検証データの生成に一方向性関数を関与させることにより、検証データから検証データ生成用データを見つけ出す困難性が増大し、悪意の第三者が真の検証データ生成用データに類似の偽の検証データ生成用データを

使って、データ改ざんをする可能性が低下する。なお、検証データから検証データ生成用データを見つけ出すことは、直列演算子列の長さが長くなればなる程、計算量的に不可能となる。

【００１９】

本発明のアドホック無線通信用検証システム及び方法によれば、第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００２０】

複数個の検証データ全部が類似している可能性は極めて低い。検証データを複数個、生成し、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されることにより、検証の正確性が向上する。

【００２１】

本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を２個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された２個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００２２】

本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっ

ている。

【００２３】

本発明のアドホック無線通信用検証システム及び方法によれば、検証データ生成用データは一方のデータ送受装置の公開鍵である。

【００２４】

検証データ生成用データが一方のデータ送受装置の公開鍵であれば、検証データの検証により、他方のデータ送受装置が受信した公開鍵が一方のデータ送受装置の公開鍵であることを検証することができる。したがって、他方のデータ送受装置から一方のデータ送受装置へ一方のデータ送受装置の公開鍵を用いた暗号通信により例えば共通鍵等を送る等して、両データ送受装置間の共通鍵による暗号通信の開設を完全に実施できる。

【００２５】

前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２６】

前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通

信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２７】

本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、公開鍵Ｋｐは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Ｋｐから共通鍵Ｋｃを第２の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２８】

本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとは

セキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Ｋｐが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Ｋｃを第２の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Ｋｃを第２の生成アルゴリズムから生成し、次に、共通鍵Ｋｃは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Ｋｃに基づく暗号によりデータを送受する。

【００２９】

各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとのセキュアな通信路とは、例えば、各ユーザの秘密鍵による相互通信により確立される。無線通信機能付き携帯端末はＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）と呼ばれるものを含む。ビジネスマンの仕事のスタイルの一例としての隠しコンピューティング（Ｈｉｄｄｅｎ　Ｃｏｍｐｕｔｉｎｇ：発明の実施の形態において詳述）が考えられている。隠しコンピューティングでは、例えばノートＰＣ等の無線通信機能付きパソコン同士で、改ざんなくデータの送受が行われることが望まれる。このようなケースにおいて、ユーザは無線通信機能付き携帯端末の検証データ出力部における検証データの対比から一方の無線通信機能付き携帯端末の公開鍵Ｋｐが途中に改ざんされることなく他方の無線通信機能付き携帯端末へ伝送されたことが検証されると、その検証を両ユーザの無線通信機能付きパソコンへ引き継がせ、両無線通信機能付きパソコンの間で共通鍵Ｋｃにより暗号通信を円滑に実施できる。

【００３０】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものである。

：アドホック無線接続により相互に接続される２個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証デー

タを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第１の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【００３１】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

録媒体。

：検証データは、視覚的又は聴覚的な検証データである。

【００３２】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【００３３】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を１個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【００３４】

本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

：第１の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【００３５】

【発明の実施の形態】

以下、発明の実施の形態について図面を参照して説明する。

図４はデータ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。暗号通信開設要求側及び被要求側をそれぞれ伝送元及び伝送先と定義し、図４では、伝送元データ送受装置をＡ、伝送先データ送受装置をＢとしている。データ完全性検証のための公開鍵の伝送元及び伝送先と、データ完全性検証後の本伝送（ほんでんそう：共通鍵を使った暗号伝送）の伝送元及び伝送先とは、一致している必要はなく、逆であってもよいし、また、データ完全性検証後の本伝送では、伝送元及び伝送先は適宜、入れ替わってもよい。

【００３６】

図４の処理を順番に説明する。

（ａ）Ａは、Ｂに暗号通信路開設要求と共に自分の公開鍵Ｋｐ、及び検証データ生成アルゴリズムを指定するＩＤ（以下、このＩＤを「ＩＤ１」と言う。）を送信する。Ａは、同時に、自分の公開鍵Ｋｐを元に検証データＸｐを生成する。

（ｂ）ＢがＡからＡの公開鍵Ｋｐとして受信したデータをＫｘとする。もし、ＡからＢへの無線伝送路においてデータの改ざんがなければ、Ｋｘ＝Ｋｐとなり、改ざんがあれば、ＫｘはＫｐとは別のものとなる。ＢはＡから受け取ったＫｘを元に、Ａより指定のあったＩＤ１の検証データ生成アルゴリズムで検証データＸｘを生成する。検証データの例は、後述の図５において詳述する。

（ｃ）Ａ、Ｂのユーザは、Ａ及びＢの表示部にそれぞれ出力表示された検証データＸｐ，Ｘｘが同一であるか否かを検証する。もし、Ｘｐ＝Ｘｘであれば、Ｋｘ＝Ｋｐを意味し、Ａ－Ｂの通信路にはデータ完全性があるとの判断を下す。

（ｄ）ＢはＡから受信した公開鍵Ｋｐを使って、共通鍵生成のための乱数値Ｒと共通鍵生成アルゴリズムを指定するＩＤ（以下、このＩＤを「ＩＤ２」と言う。）とを暗号化して、Ａへ送信する。ＩＤ２については、Ａ，Ｂが同一の通信ソフトを使用する等、ＩＤ２が固定されているならば、ＩＤ１と同様に、Ａ－Ｂ間の伝送は省略できる。Ｂは、同時に乱数値Ｒから共通鍵生成アルゴリズムを用いて共通鍵Ｋｃを生成する。

（ｅ）ＡはＢから受信した暗号化された乱数値Ｒを、公開鍵Ｋｐに対応する秘密

鍵を使って復号し、乱数値ＲとＩＤ２とを得、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムを用いて共通鍵Ｋｃを生成する。

（ｆ）以降、Ａ－Ｂは、共通鍵Ｋｃに基づく暗号化通信によりデータを送受する。

【００３７】

Ａ，Ｂの検証データ出力部に表示する検証データは検証データ生成用データそのもの、例えばＡの公開鍵そのものであってもよい。すなわち、Ａ，Ｂの検証データ生成用データに、Ａの公開鍵がビット表示される。しかし、数値では、読み取り難いので、公開鍵の数値表示を画像表示へ変換してもよい。 図５は検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す。検証データはデータ送受装置２０（図６）の検証画像表示部２７に視覚表示される。検証データ生成用データがＡの公開鍵であるとして、公開鍵をＬＳＢからＭＳＢまでを等しいビット数の区域に順番に区切り、横軸を区域、縦軸を各区域の数量とするヒストグラムで、検証データが表されている。もし、Ａの公開鍵Ｋｐが、伝送路の途中で悪意の第三者により成りすましが行われていなければ、ＢがＡより受信した検証データ生成用データＫｘは、検証データ生成用データＫｐに等しいので、Ｘｘ＝Ｘｐとなる。したがって、Ａ及び／又はＢのユーザ、又は信頼できる他の検証者は、Ａ，Ｂの表示部を直接、見て、Ａ，Ｂの表示部に表示されているＸｐ及びＸｘを対比（比較）し、両者が一致していれば、ＡからＢへＡの公開鍵がそのまま伝送されて来たと判断し、すなわちデータ完全性があると判断し、両者が不一致であれば、ＡからＢへの伝送途中にデータの改ざんがあったと判断する。

【００３８】

しかし、人間の認識能力の精度は必ずしも高くなく、図５のようなヒストグラムの比較画像を単純に生成しただけではハミングディスタンスの小さい類似公開鍵との違いを検出できない場合がある。そこで、公開鍵に対してハッシュ関数等の一方向性関数を適用して所定のデータへ変換し、それをヒストグラム等の検証画像の表示を行ってもよい。この場合、成りすましを行おうとする第三者が類似するデータを出力する別の公開鍵を求めようとしても、離散対数問題を解くこと

になり計算量的に不可能である。ただし、作成する検証画像の情報量が公開鍵のビットサイズに比べて極めて小さい場合、全数探索によって破られる可能性がある。そのような条件下では、すでに一方向性関数を適用したデータに対してさらに一方向性関数を適用して新たなデータを算出したり、別の一方向性関数を公開鍵に適用して新たなデータを算出したりして、別の検証画像を生成する。この操作を繰り返すことで、複数の検証画像を生成することができ、これを用いることで成りすましに対する強度をあげることができる。

【００３９】

検証データは、ヒストグラムのような画像に限定されず、文字データの表示や音階の変化などを用いたり、それらの複数のデータを組み合わせたりして、ユーザに対して提示したりしてもよい。聴覚的な検証データとしては、図５のヒストグラムの縦軸方向の値を音の高低又は音色に対応させ、図６の横軸方向の左の区域から順番に所定時間ごとに各区域の値に対応する音を出力する。また、検証データを視覚表示器と放音手段としてのスピーカとの両方から出力させるようにしてもよい。

【００４０】

図６～図８は一方向性関数を使用して検証データ生成用データから検証データを生成する方式をそれぞれ示している。データＤ１は検証データ生成用データを意味し、データＤ２，Ｄ３，Ｄ４，・・・は検証データを意味する。また、各一方向性関数は、演算子として機能し、入力に作用して、演算結果を出力する。一方向性関数は例えばハッシュ関数（Ｈａｓｈ　Ｆｕｎｃｔｉｏｎ）である。

【００４１】

図６では、１回目は検証データ生成用データとしてのデータＤ１に一方向性関数Ｆを作用させ、データＤ２を得る。２回目は、データＤ２に同一の一方向性関数Ｆを作用させ、すなわち、一方向性関数Ｆを含むループを形成し、データＤ３を得る。以降、ループ処理を繰り返し、Ｄ４、Ｄ５、・・・を得る。所定回数のループを繰り返した後、最終的な演算結果をＤｎとし、このＤｎを検証データとし、この検証データをデータ送受装置２０（図１０）の検証画像表示部２７に視覚表示する。最終的な演算結果Ｄｎのみデータ送受装置２０の検証画像表示部２

７に視覚表示するだけでなく、Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部をデータ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させることにし、表示されたそれぞれについて対比してもよい。複数の検証データを対比することにより、たとえそれらの１個の検証データについての一致・不一致の判定が紛らわしくても、対比される複数の検証データのすべてについて一致・不一致の判定が紛らわしくなる可能性は極めて小さく、データ改ざんについての検証の正確性を向上できる。

【００４２】

なお、Ｄ２，Ｄ３，Ｄ４，・・・の全部でなく、特定の幾つかのみを対比する場合に、その幾つかについての組み合わせ（Ｓｕｂｓｅｔ）を適宜、変更するようにしておくことにより、悪意の第三者の攻撃に対する防護強度は高くなる。

【００４３】

図７では、相互に異なる複数個の一方向性関数Ｆ，Ｇ，Ｈ，・・・を用意し、共通のデータＤ１に各一方向性関数Ｆ，Ｇ，Ｈ，・・・を作用させ、各演算結果Ｄ２，Ｄ３，Ｄ４，・・・を得る。Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部を検証データとして、データ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。

【００４４】

図８では、相互に異なる複数個の一方向性関数Ｆ，Ｇ，Ｈ，・・・を用意する。１回目は検証データ生成用データとしてのデータＤ１に一方向性関数Ｆを作用させ、データＤ２を得る。２回目は、データＤ２に一方向性関数Ｇを作用させ、データＤ３を得る。こうして、次々に前段の演算結果に次段の一方向性関数を作用させ、複数個のＤ２，Ｄ３，Ｄ４，・・・を得る。Ｄ２，Ｄ３，Ｄ４，・・・の特定の幾つか又は全部を検証データとして、データ送受装置２０の検証画像表示部２７に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。なお、図６における複数個対比の方式は、図８の方式において、相互に異なる一方向性関数を使用する代わりに同一の一方向性関数Ｆを使用した特殊の例と考えることができる。

【００４５】

図９は図６～図８の処理を組み合わせて検証データを求める方式を示すブロック図である。図６～図９の検証データ演算方式をそれぞれタイプ（Ｔｙｐｅ）１，２，３と定義している。図８の左端に検証データ生成用データが入力され、図８の右端に検証データが出力される。図９の配列例は一例である、タイプ１，２，３から２個以上のタイプを選択し、それらを任意の順に並べて、検証データ生成用データを得ることができる。

【００４６】

図１０はデータ送受装置２０のブロック図である。データ送受装置２０は、場合により伝送元Ａになったり、伝送先Ｂになったするので、伝送元としての構成と伝送先としての構成を兼備している。データ送受装置２０がＡである場合には、伝送検証部２４は、自分の公開鍵を検証画像生成部２６へ出力し、また、データ送受装置２０がＢである場合には、通信部２５においてＡからの送受信データ３１として受信したＡの公開鍵は伝送検証部２４を経由して検証画像生成部２６へ送られる。検証画像生成部２６は伝送検証部２４から受けた公開鍵から検証データを生成し、生成された検証データは検証画像表示部２７に表示される。Ａ，Ｂの所有者等のユーザは、アドホック無線接続されている２個のデータ送受装置２０の検証画像表示部２７における検証データを対比し、一致及び不一致を調べ、その結果を検証結果入力部２８に入力する。ユーザからの検証結果入力部２８への入力結果は伝送検証部２４へ通知され、伝送検証部２４は、両検証データが相互に一致しているとの通知を受けた場合には、ＡからＢへアドホック無線接続の伝送路を介して伝送した公開鍵についてデータ完全性があると判断する。次に、データ送受装置２０がＢである場合には、乱数生成部３４において乱数値が生成され、共通鍵生成部３３では、乱数生成部３４において生成された乱数値からＩＤ２の共通鍵生成アルゴリズムにより共通鍵を生成する。一方、乱数生成部３４が生成した乱数値及びＩＤ２が復号化・暗号化実施部３２においてＡの公開鍵に基づいて暗号化され、その暗号データＤｃが送受信データ３１を介してＡへ送られる。また、乱数値ＲからＩＤ２の生成アルゴリズムに基づいて共通鍵を生成し、それを鍵保存部３５に保存する。データ送受装置２０がＡである場合には、Ｂから伝送されて来た暗号データＤｃの送受信データ３１を復号化・暗号化実施

部３２において自分の秘密鍵により復号し、乱数値Ｒ及びＩＤ２を得、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムに基づいて共通鍵を生成し、該共通鍵を鍵保存部３５に保存する。以降は、データを送信する場合は、鍵保存部３５から共通鍵を引き出して、該共通鍵に基づいて送信データを復号化・暗号化実施部３２において暗号化し、送受信データ３１として相手方へ送信する。データを受信する場合は、受信した暗号化され送受信データ３１を復号化・暗号化実施部３２において復号し、平データをハードディスク（図示せず）等に保存したり、所定の処理を行ったりする。

【００４７】

図１１は伝送元Ａ側の通信処理のフローチャートである。公開鍵Ｋｐを送信し（Ｓ４０）、該公開鍵ＫｐからＩＤ１の検証データ生成アルゴリズムにより検証データＸｐを生成し（Ｓ４２）、検証データＸｐを検証画像表示部２７に出力する（Ｓ４４）。Ｓ４６では、自分の検証データＸｐと伝送先Ｂの検証データＸｘとを対比して、同一と判断されれば、Ｓ４８へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、伝送先Ｂからの乱数値Ｒの受信を待ち（Ｓ４８）、Ｓ５０において、乱数値Ｒを受信したと判断すると、Ｓ５２へ進み、乱数値受信待ち時間が所定時間経過したにもかかわらず、乱数値Ｒの受信のないときは、エラーとして該プログラムを終了する。Ｓ５２では、伝送先Ｂからの乱数値Ｒの暗号データを前記公開鍵Ｋｐに対応の自分の秘密鍵で復号して、乱数値Ｒを得る。Ａ，Ｂのデータ送受装置間では複数個の共通鍵生成アルゴリズムについてそれぞれＩＤが予め取り決められており、送信先Ｂにおいて今回の共通鍵生成アルゴリズムとして採用されたＩＤ（例では、ＩＤ２）が乱数値Ｒと一緒に伝送先Ｂから伝送元Ａへ送信されて来ている。こうして、Ｓ５６では、乱数値ＲからＩＤ２の共通鍵生成アルゴリズムに基づいて送信先Ｂとの通信用の共通鍵を生成し、以降、該共通鍵を用いてＢと暗号化通信を開始する（Ｓ５８）。

【００４８】

図１２は伝送先Ｂ側の通信処理のフローチャートである。伝送元Ａから公開鍵Ｋｘを受信する（Ｓ６０）。この受信した公開鍵は、Ａ，Ｂ間の伝送路に悪意の

第三者が介在していて改ざんされている可能性があるかもしれないので、Ｋｃではなく、Ｋｘと表現することにする。次に、送信元Ａから公開鍵Ｋｐと一緒に送られて来たＩＤ１で指定される検証データ生成アルゴリズムによりＫｘから検証データＸｘを生成し（Ｓ６２）、検証データＸｘを検証画像表示部２７に出力する（Ｓ６４）。Ｓ６６では、自分の検証データＸｘと伝送元Ａの検証データＸｐとを対比して、同一と判断されれば、Ｓ６８へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、乱数値Ｒを生成し（Ｓ６８）、乱数値Ｒと、複数個の共通鍵生成アルゴリズムの中から、今回、選択した共通鍵生成アルゴリズムのＩＤとしてのＩＤ２とを送信元Ａの公開鍵により暗号化したデータを送信元Ａへ送信し（Ｓ７０）、ＩＤ２の共通鍵生成アルゴリズムに従って共通鍵Ｋｃを生成し（Ｓ７２）、以降、該共通鍵を用いてＡと暗号化通信を開始する（Ｓ７４）。

【００４９】

図１３は隠れコンピューティングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。隠れコンピューティング（Hidden Computing）とは、ユーザは、コンピュータを鞄等に納め、手元のＰＤＡ（携帯情報端末：Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の携帯機器から無線通信等を利用して該コンピュータを遠隔操作する利用形態を意味する。ＰＤＡ８０ａ等に装備されている８２は通信デバイスである。上記に述べたような公開鍵のデータの完全性を確認できるシステムを装備していない機器（＝鞄８６ａ，８６ｂの中のノートパソコン８８ａ，８８ｂ）間でアドホック無線通信を行う場合において、これらノートパソコン８８ａ，８８ｂと事前にセキュアな通信路９０ａ，９０ｂを確保している暗号通信路開設プロトコルを実装したＰＤＡ８０ａ，８０ｂを用いて、間接的に暗号通信路を開設する。なお、ＰＤＡとノートパソコンとの間のセキュアな通信路は、例えば両者間で事前に取り決められている共通鍵による暗号通信により達成される。図１３においてまず手順（ａ）で通信路８４をＰＤＡ８０ａ，８０ｂ間で開設して、一方のＰＤＡの公開鍵を他方のＰＤＡへ伝送して、該公開鍵のデータ完全性を検証する。次に、手順（ｂ）においてＰＤＡ８０ａ，８０ｂ間のデータ完全性検証を、それぞれのＰ

ＤＡ８０ａ，８０ｂとセキュアな通信路９０ａ，９０ｂにより接続されているノートパソコン８８ａ，８８ｂへ継承する。この継承は、具体的には、ＰＤＡ８０ａ，８０ｂ間でデータ完全性を検証された公開鍵をセキュアな通信路９０ａ，９０ｂを介してノートパソコン８８ａ，８８ｂを伝送することにより達成される。以降、ノートパソコン８８ａ，８８ｂは、両者間の通信路９２を介して共通鍵を共有した後、該共通鍵による暗号でデータを送受する。

【図面の簡単な説明】

【図１】

送信元Ａと送信先Ｂとが気付かないままで両者の間に悪意の第三者Ｃが介在する余地を示す図である。

【図２】

悪意の第三者が図１のＣの位置に入り込む手口の一例の第１の部分を示す図である。

【図３】

悪意の第三者が図１のＣの位置に入り込む手口の一例の第２の部分を示す図である。

【図４】

データ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。

【図５】

検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す図である。

【図６】

一方向性関数を使用して検証データ生成用データから検証データを生成する第１の方式を示す図である。

【図７】

一方向性関数を使用して検証データ生成用データから検証データを生成する第２の方式を示す図である。

【図８】

一方向性関数を使用して検証データ生成用データから検証データを生成する第３の方式を示す図である。

【図９】

図６～図８の処理を組み合わせて検証データを求める方式を示すブロック図である。

【図１０】

データ送受装置のブロック図である。

【図１１】

伝送元Ａ側の通信処理のフローチャートである。

【図１２】

伝送先Ｂ側の通信処理のフローチャートである。

【図１３】

隠れコンピューティングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。

【符号の説明】

１０　　アドホック無線通信システム

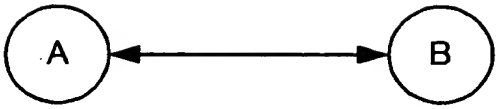
８０ａ，８０ｂ　　ＰＤＡ（無線通信機能付き携帯情報端末）

８８ａ，８８ｂ　　ノートパソコン（無線通信機能付きパソコン）

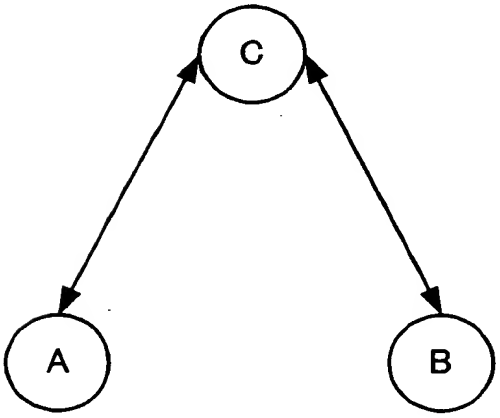
【書類名】　　図面

【図１】

(a)

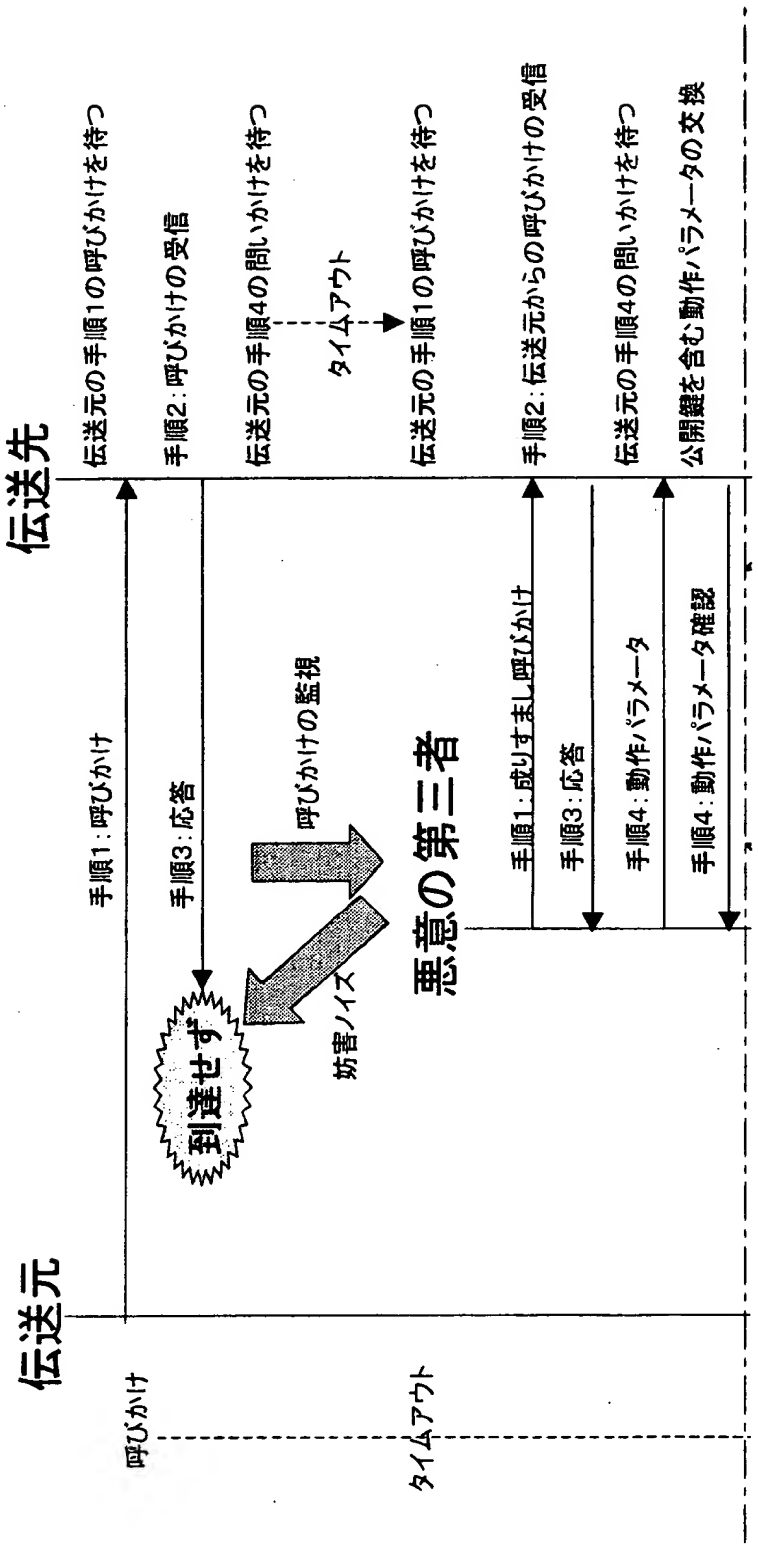


(b)

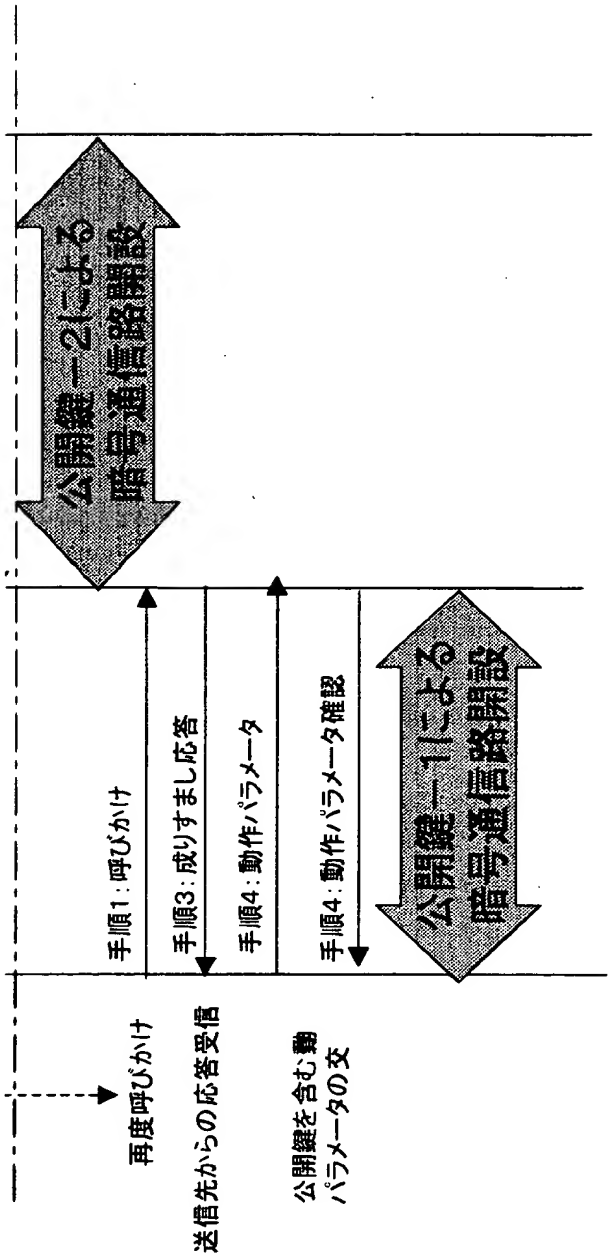


出証特２０００－３１０７２８１

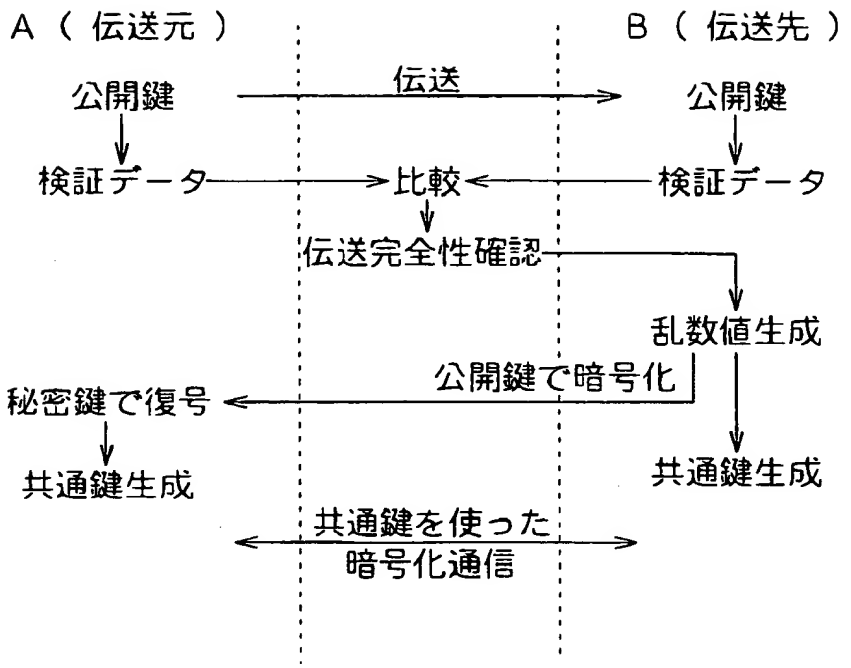
【図２】


伝送先
伝送元の手順1の呼びかけを待つ
手順2：呼びかけの受信
伝送元の手順4の間いかけを待つ
タイムアウト
伝送元の手順1の呼びかけを待つ
手順2：伝送元からの呼びかけの受信
伝送元の手順4の間いかけを待つ
公開鍵を含む動作パラメータの交換
手順1：呼びかけ
手順3：応答
呼びかけの監視
悪意の第三者
手順1：成りすまし呼びかけ
手順3：応答
手順4：動作パラメータ
手順4：動作パラメータ確認
到達せず
妨害ノイズ
伝送元
呼びかけ
タイムアウト

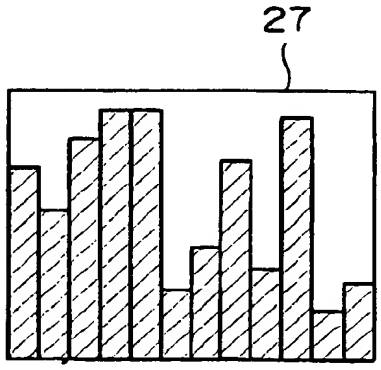
【図３】


公開鍵－2による
暗号通信路開設
公開鍵－1による
暗号通信路開設
手順1：呼びかけ
手順3：成りすまし応答
手順4：動作パラメータ
手順4：動作パラメータ確認
再度呼びかけ
送信先からの応答受信
公開鍵を含む動
パラメータの交

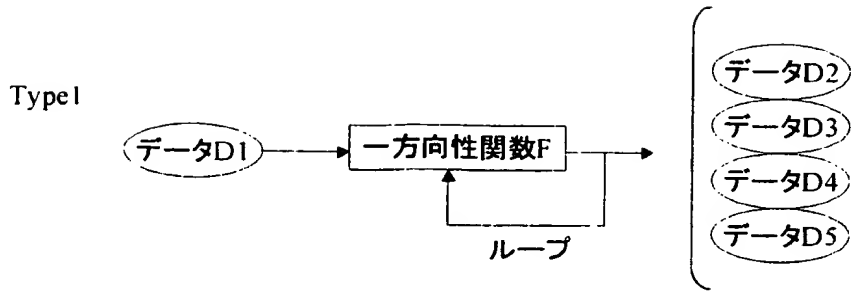
【図４】


A（伝送元）
B（伝送先）
公開鍵
伝送
公開鍵
検証データ
比較
検証データ
伝送完全性確認
乱数値生成
公開鍵で暗号化
秘密鍵で復号
共通鍵生成
共通鍵生成
共通鍵を使った
暗号化通信

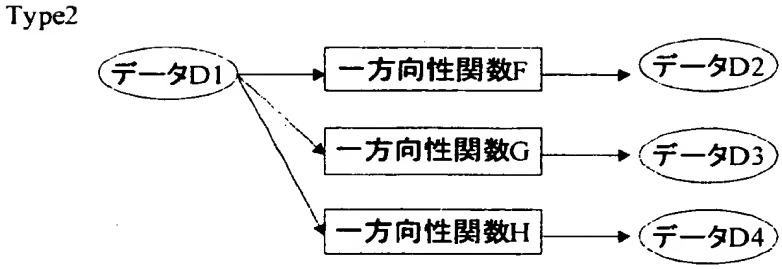
【図５】


27

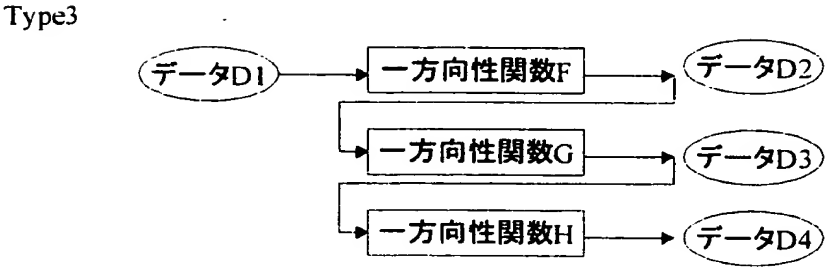
【図６】



【図７】

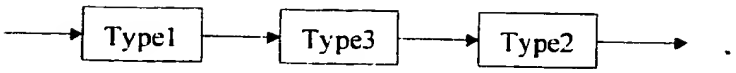


【図８】

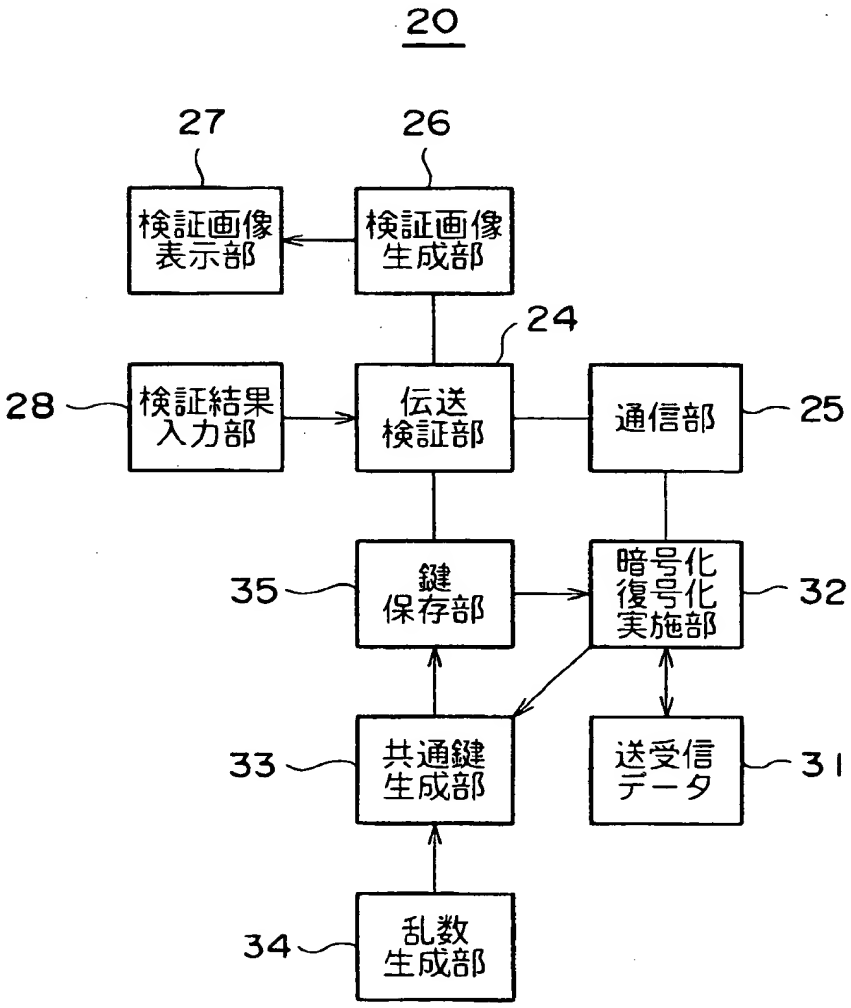


出証特２０００－３１０７２８１

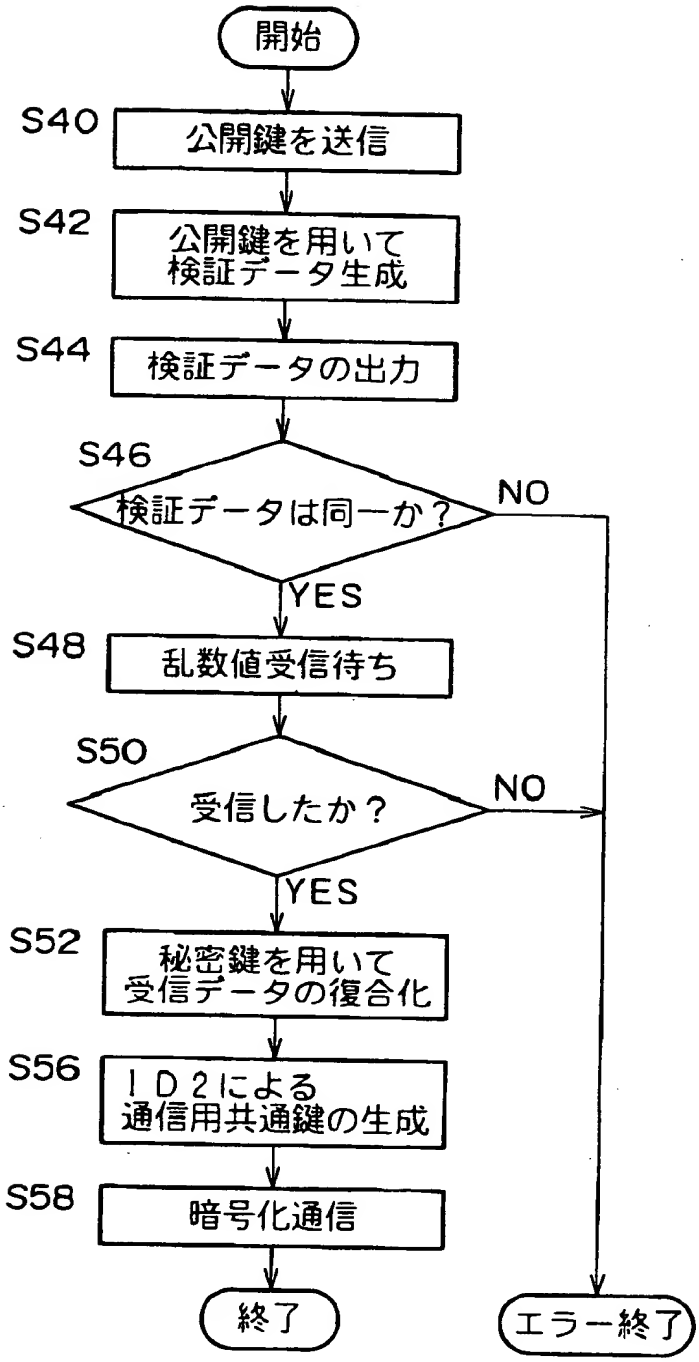
【図９】


Type1
Type3
Type2

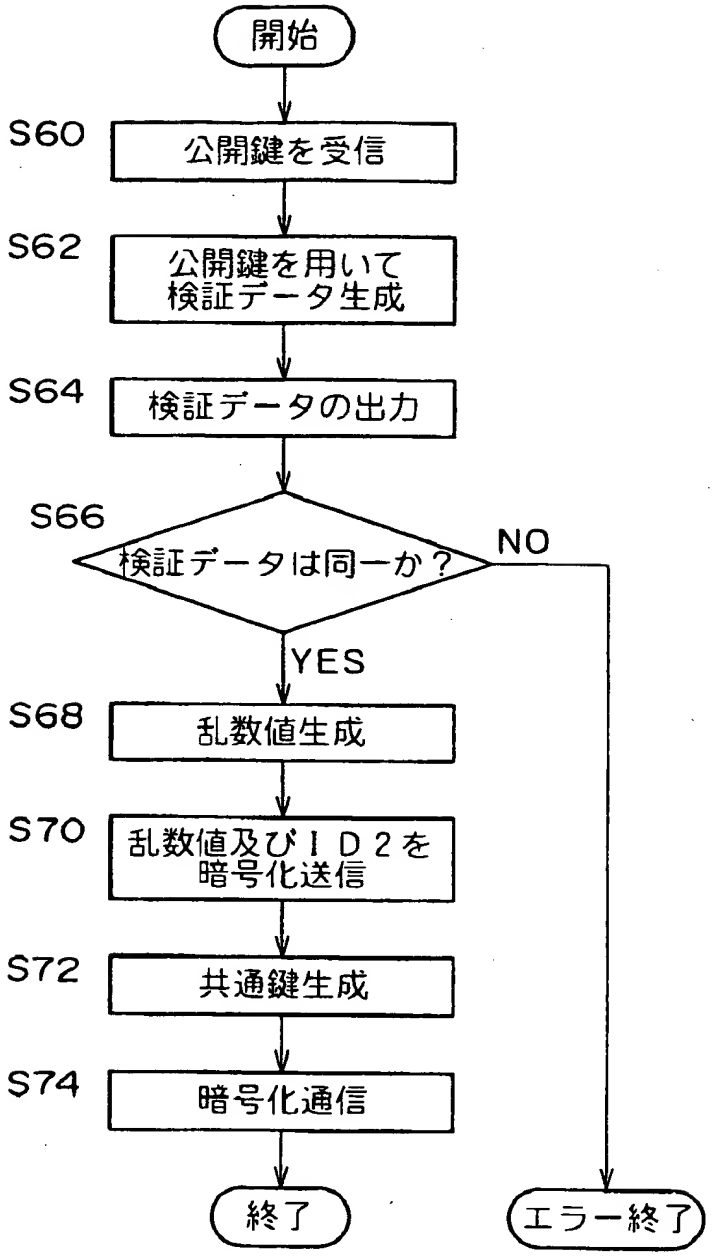
【図１０】


20
27
26
検証画像表示部
検証画像生成部
24
28
検証結果入力部
伝送検証部
通信部
25
35
鍵保存部
暗号化復号化実施部
32
33
共通鍵生成部
送受信データ
31
34
乱数生成部

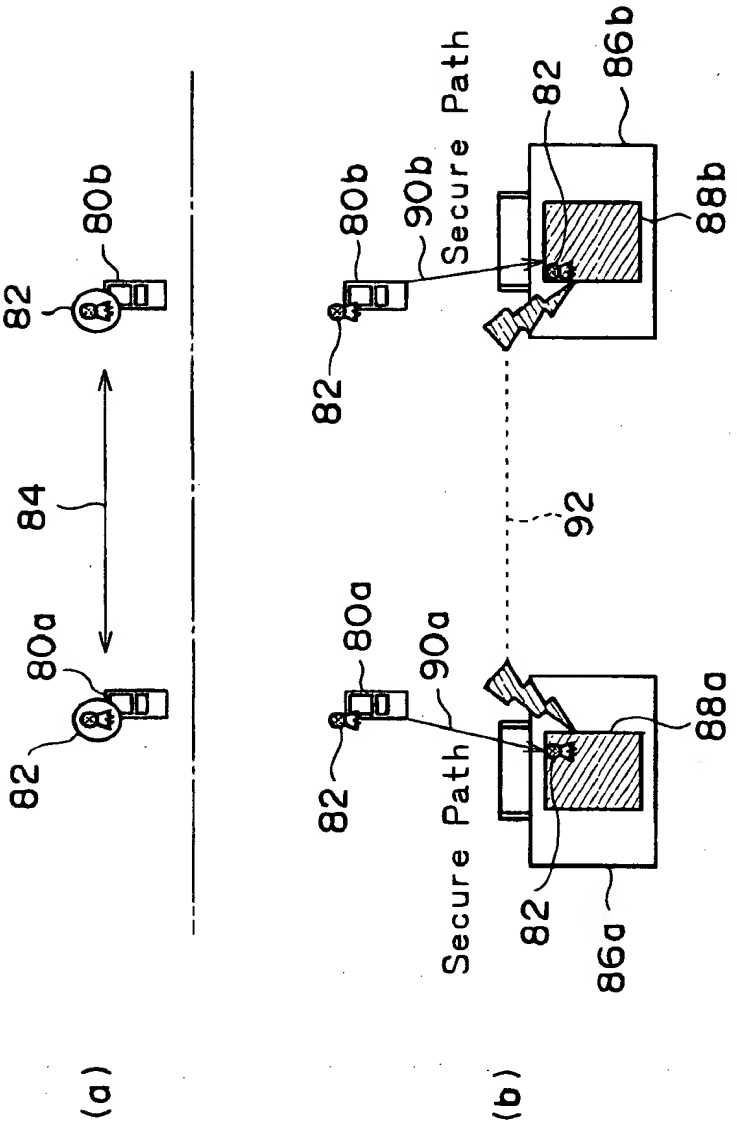
【図１１】


開始
S40
公開鍵を送信
S42
公開鍵を用いて
検証データ生成
S44
検証データの出力
S46
検証データは同一か？
NO
YES
S48
乱数値受信待ち
S50
受信したか？
NO
YES
S52
秘密鍵を用いて
受信データの復合化
S56
ＩＤ２による
通信用共通鍵の生成
S58
暗号化通信
終了
エラー終了

【図１２】


開始
S60
公開鍵を受信
S62
公開鍵を用いて
検証データ生成
S64
検証データの出力
S66
検証データは同一か？
NO
YES
S68
乱数値生成
S70
乱数値及びＩＤ２を
暗号化送信
S72
共通鍵生成
S74
暗号化通信
終了
エラー終了

【図１３】


80b
82
84
80a
82
(a)
80b
90b
Secure Path
82
86b
82
88b
92
80a
90a
82
Secure Path
88a
82
86a
(b)

【書類名】　　要約書

【要約】

【課題】　アドホック無線接続によるデータ送受信においてデータ完全性を簡単に検証する。

【解決手段】　暗号通信路開設を要求する要求元及び要求先をそれぞれ伝送元Ａ及び伝送先Ｂと定義する。ＡとＢとの間には、予め検証データ生成アルゴリズムＩＤ１が取り決められている。Ａは、Ｂへ例えばＡの公開鍵Ｋｐを伝送するとともに、ＩＤ１によりＫｐから検証データＸｐを生成し、それを自分の検証画像表示部２７へ出力する。Ｂは、ＡからＫｐとして伝送されて来たデータＫｘを受信し、ＩＤ１によりＫｘから検証データＸｘを生成し、それを自分の検証画像表示部２７へ出力する。検証者は、Ａ，Ｂの検証画像表示部２７のＸｐ，Ｘｘが一致しているならば、データ完全性があると判断する。

【選択図】　　図４

認定・付加情報

特許出願の番号	特願２０００－１８４６９７
受付番号	５００００７６８３０９
書類名	特許願
担当官	佐藤　一博　　１９０９
作成日	平成１２年　７月３１日

＜認定情報・付加情報＞

【提出日】　平成12年 6月20日

【特許出願人】

【識別番号】　390009531

【住所又は居所】　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

【識別番号】　100086243

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名又は名称】　市位　嘉宏

【代理人】

【識別番号】　100106699

【住所又は居所】　神奈川県大和市下鶴間１６２３番１４　日本アイ・ビー・エム株式会社大和事業所内

【氏名又は名称】　渡部　弘道

【復代理人】　申請人

【識別番号】　100060726

【住所又は居所】　東京都中央区日本橋２丁目１番１号　櫻正宗ビル９階

【氏名又は名称】　石山　博

【選任した復代理人】

次頁有

認定・付加情報（続き）

【識別番号】　100085408
【住所又は居所】　東京都中央区日本橋２丁目１番１号　櫻正宗ビル９階
【氏名又は名称】　山崎　隆

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　２０００年　５月１６日
［変更理由］　名称変更
住　所　　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　　インターナショナル・ビジネス・マシーンズ・コーポレーション